

Gröbner basis in Boolean rings is not polynomial-space

Mark van Hoeij*
Florida State University
Tallahassee, FL 32306-3027, USA

February 27, 2015

Abstract

We give an example where the number of elements of a Gröbner basis in a Boolean ring is not polynomially bounded in terms of the bitsize and degrees of the input.

1 Boolean Rings

Let $R_n = \mathbb{F}_2[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n]$ where $\mathbb{F}_2 = \mathbb{Z}/(2)$. If $S \subseteq R_n$ then (S) denotes the ideal in R_n generated by S , and $\text{Sol}(S) \subseteq K^{3n}$ denotes the solution set of S , where K is the algebraic closure of \mathbb{F}_2 . Let

$$S_n := \{c^2 - c \mid c \in \{x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n\}\}.$$

$R_n^b := R_n/(S_n)$ is a *Boolean ring*, which means $r^2 = r$ for all r in R_n^b . If I is an ideal in R_n , then $S_n \subseteq I$ if and only if I is radical and $\text{Sol}(I) \subseteq \mathbb{F}_2^{3n}$.

Ideals in R_n that contain S_n are in 1-1 correspondence with ideals in R_n^b . Thus, Gröbner basis in R_n^b is equivalent to: Gröbner basis in R_n restricted to ideals that contain S_n . We will show with an example that this is not polynomial-space.

2 Example

Let

$$\begin{aligned} L_n &= \{x_i y_i + x_i + y_i - z_i \mid i = 1, \dots, n\} \\ T_n &= \{x_i z_i - x_i \mid i = 1, \dots, n\} \cup \{y_i z_i - y_i \mid i = 1, \dots, n\} \\ P_n &= \left\{ \prod_{i=1}^n c_i \mid c_1 \in \{x_1, y_1, z_1\}, \dots, c_n \in \{x_n, y_n, z_n\} \right\}. \end{aligned}$$

*Supported by NSF grant 1319547

Let $G_n := S_n \cup L_n \cup T_n \cup P_n$ and $H_n = S_n \cup L_n \cup \{z_1 z_2 \cdots z_n\} \subseteq G_n$.

Lemma 2.1. $(H_n) = (G_n)$.

Proof: Both are radical so it suffices to show $\text{Sol}(H_n) = \text{Sol}(G_n)$. If $x, y \in \mathbb{F}_2$ and $z = xy + x + y$ then $z = 0 \iff x = 0 \wedge y = 0$. It follows that $\text{Sol}(H_n)$ is the set of all $(x_1, y_1, z_1, \dots, x_n, y_n, z_n)$ for which: $x_i, y_i \in \mathbb{F}_2$, $z_i = x_i y_i + x_i + y_i$, and $\exists_i x_i = y_i = 0$. These are solutions of $G_n \supseteq H_n$ as well. \square

Lemma 2.2. If $n > 1$ then G_n is a reduced Gröbner basis of (G_n) w.r.t. any admissible total-degree ordering.

Let ord be an admissible total-degree ordering. It is easy to check that G_n is reduced when $n > 1$, which means that for any $f, g \in G_n$ with $f \neq g$, the ord -leading monomial of f is not divisible by the ord -leading monomial of g . It remains to show that G_n is a Gröbner basis.

Proof: Let B_n be the set of all monomials that are not divisible by the leading monomial of an element of G_n and let V_n be the \mathbb{F}_2 -vector space with basis B_n . The natural map $V_n \rightarrow R_n/(G_n)$ is always surjective and is bijective if and only if G_n is a Gröbner basis. So it suffices to show that V_n and $R_n/(G_n)$ have the same dimension.

Since (G_n) is radical, $\dim R_n/(G_n)$ is the number of solutions of G_n , which is $4^n - 3^n$ (see the proof of Lemma 2.1). This equals the number of elements of

$$B_n = \left\{ \prod_{i=1}^n c_i \mid c_1 \in \{1, x_1, y_1, z_1\}, \dots, c_n \in \{1, x_n, y_n, z_n\} \right\} - P_n.$$

\square

To check the lemmas for a value of n , copy this in Maple:

```
n := 4;
vars := {seq(op({x[i], y[i], z[i]}), i=1..n)};
S := {seq(c^2-c, c=vars)};
L := {seq(x[i]*y[i] + x[i] + y[i] - z[i], i=1..n)};
H := S union L union {mul(z[i], i=1..n)};
G := Groebner[Basis](H, tdeg(op(vars)), characteristic = 2);
nops(H) = 4*n+1, nops(G) = 6*n + 3^n;
```

Lemma 2.3. If $n > 1$ then any total-degree ordered Gröbner basis of (G_n) has at least $6n + 3^n$ elements.

Proof: G_n has $|S_n| + |L_n| + |T_n| + |P_n| = 3n + n + 2n + 3^n = 6n + 3^n$ elements. Gröbner bases are not unique, but any Gröbner basis has at least as many elements as a reduced Gröbner basis. \square

Theorem 2.4. Gröbner basis in Boolean rings is not polynomial-space.

Proof: Let $n > 1$. H_n has $4n + 1$ elements, whose degrees and bitsizes are bounded by a polynomial in n . But a total-degree ordered Gröbner basis does not fit in polynomial-space because it has at least $6n + 3^n$ elements. \square

3 Comments

The example was constructed by converting $\exists_{i \in \{1, \dots, n\}} x_i = y_i = 0$ to an ideal. Converting this to a Gröbner basis increases the size exponentially.

Gröbner basis techniques are sometimes used for Boolean expressions. Examples where this is beneficial can be found in Table 3 in [1].

The previous version of this preprint used the phrase P-SPACE to denote polynomial-space complexity because PSPACE is only for decision procedures (e.g.: ideal membership in Boolean rings is in PSPACE). But P-SPACE is not standard terminology, so it is replaced by polynomial-space in this version.

References

- [1] M. Brickenstein, A. Dreyer. *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*, J. Symbolic Computation **44** 1326–1345 (2009)
- [2] D. Cox, J. Little, D. O’Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. ISBN 0-387-94680-2 (1997)
- [3] Y. Sato, S. Inoue, A. Suzuki, K. Nabeshima, K. Sakai. *Boolean Gröbner basis*. J. Symbolic Computation **46** 622–632 (2011)
- [4] Q-N. Tran. *A P-SPACE Algorithm for Groebner Bases Computation in Boolean Rings*. Proc. WASET, Vol. 35 (2008)